Fig. 1

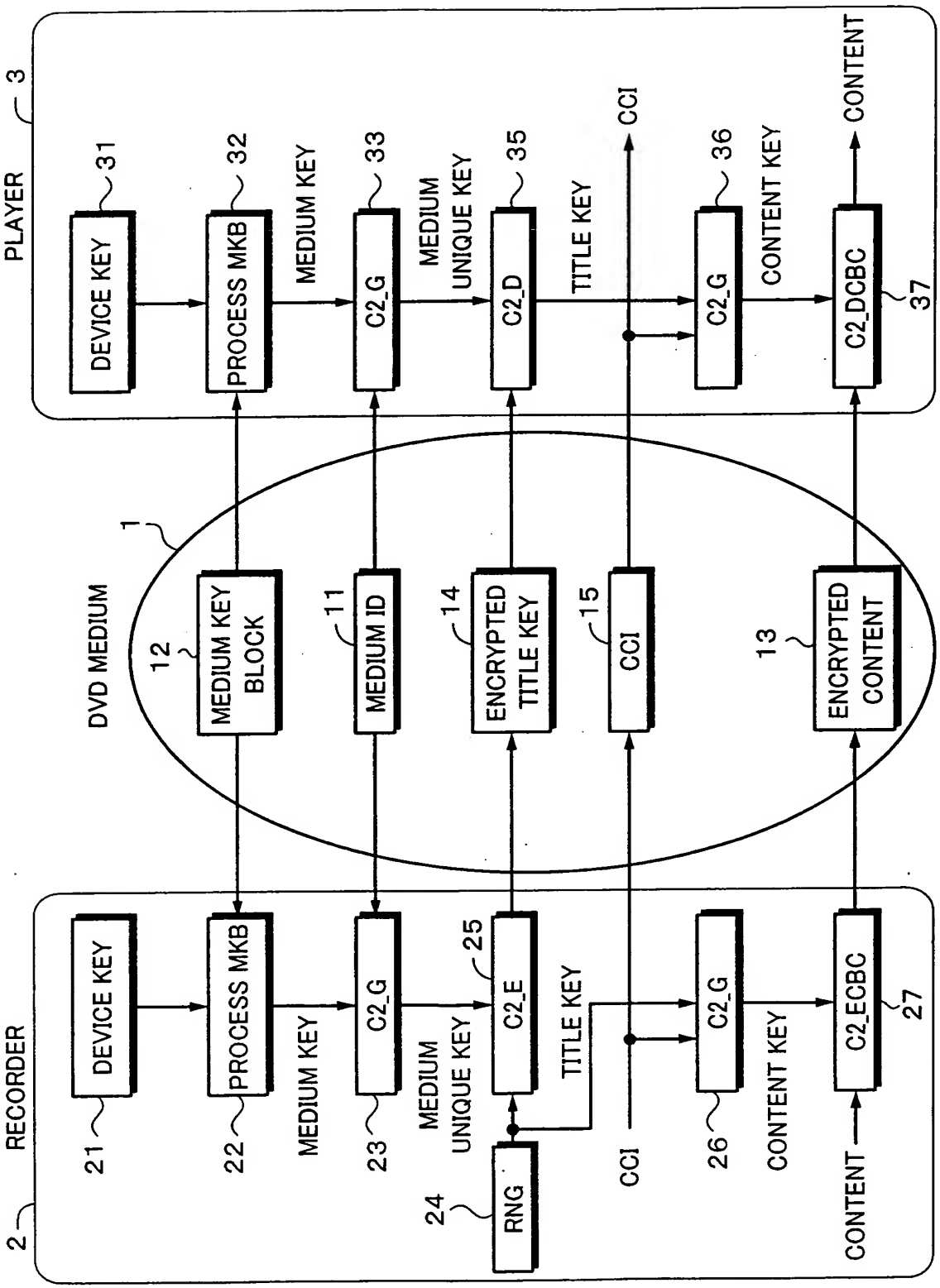

PLAYER
3
DEVICE KEY
31
PROCESS MKB
32
MEDIUM KEY
C2_G
33
MEDIUM UNIQUE KEY
C2_D
35
TITLE KEY
CCI
C2_G
36
CONTENT KEY
C2_DCBC
37
CONTENT
DVD MEDIUM
1
MEDIUM KEY BLOCK
12
MEDIUM ID
11
ENCRYPTED TITLE KEY
14
CCI
15
ENCRYPTED CONTENT
13
RECORDER
2
DEVICE KEY
21
PROCESS MKB
22
MEDIUM KEY
C2_G
23
MEDIUM UNIQUE KEY
C2_E
25
TITLE KEY
RNG
24
CCI
C2_G
26
CONTENT KEY
C2_ECBC
27
CONTENT

Fig. 2

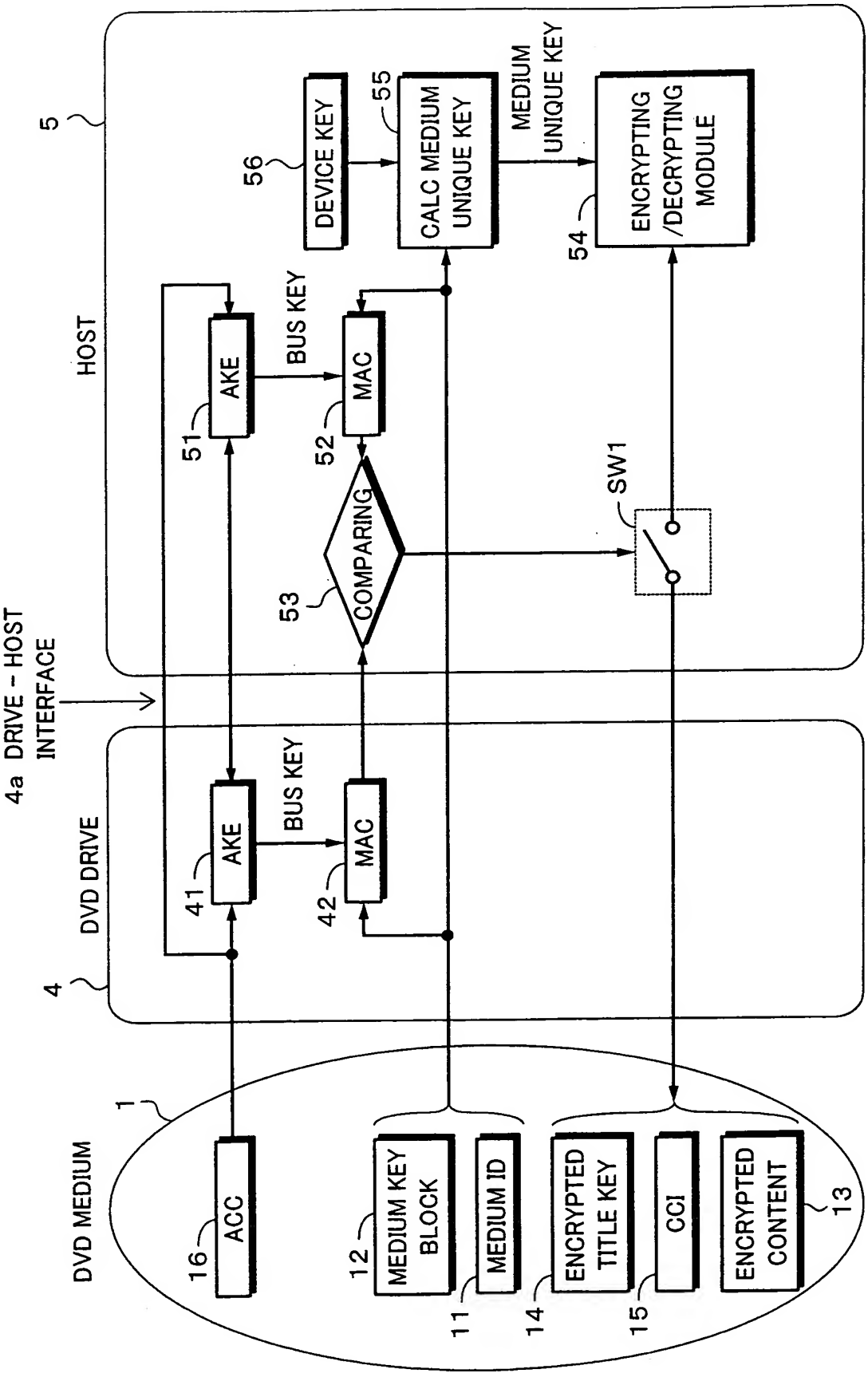

DVD MEDIUM
1
ACC
16
MEDIUM KEY BLOCK
12
MEDIUM ID
11
ENCRYPTED TITLE KEY
14
CCI
15
ENCRYPTED CONTENT
13
4
DVD DRIVE
4a DRIVE - HOST INTERFACE
AKE
41
BUS KEY
MAC
42
5
HOST
AKE
51
BUS KEY
MAC
52
COMPARING
53
SW1
DEVICE KEY
56
CALC MEDIUM UNIQUE KEY
55
MEDIUM UNIQUE KEY
ENCRYPTING /DECRYPTING MODULE
54

Fig. 3

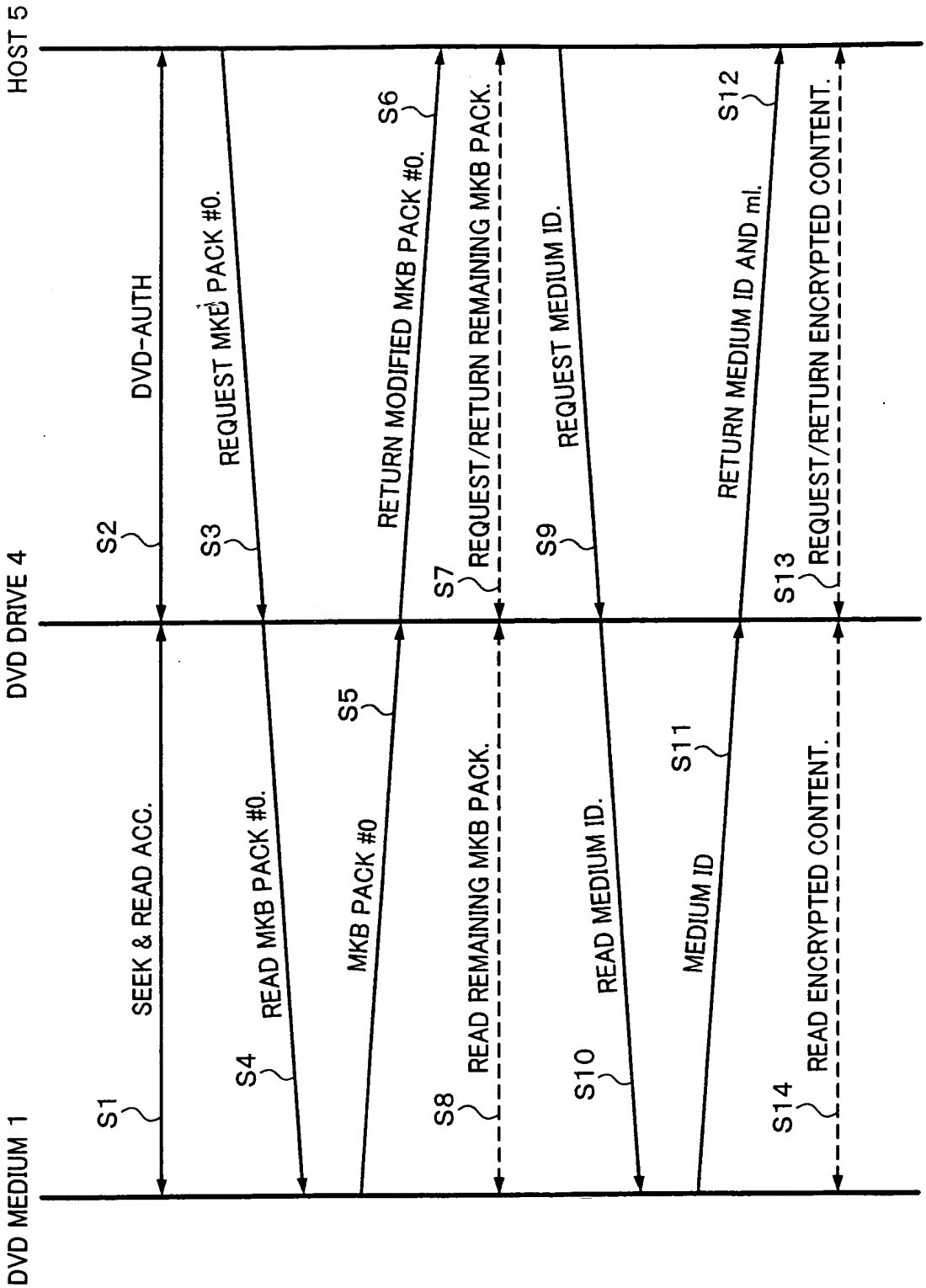

HOST 5
DVD DRIVE 4
DVD MEDIUM 1
DVD-AUTH
S2
REQUEST MKB PACK #0.
S3
RETURN MODIFIED MKB PACK #0.
S6
REQUEST/RETURN REMAINING MKB PACK.
S7
REQUEST MEDIUM ID.
S9
RETURN MEDIUM ID AND mi.
S12
REQUEST/RETURN ENCRYPTED CONTENT.
S13
SEEK & READ ACC.
S1
READ MKB PACK #0.
S4
MKB PACK #0
S5
READ REMAINING MKB PACK.
S8
READ MEDIUM ID.
S10
MEDIUM ID
S11
READ ENCRYPTED CONTENT.
S14

Fig. 4

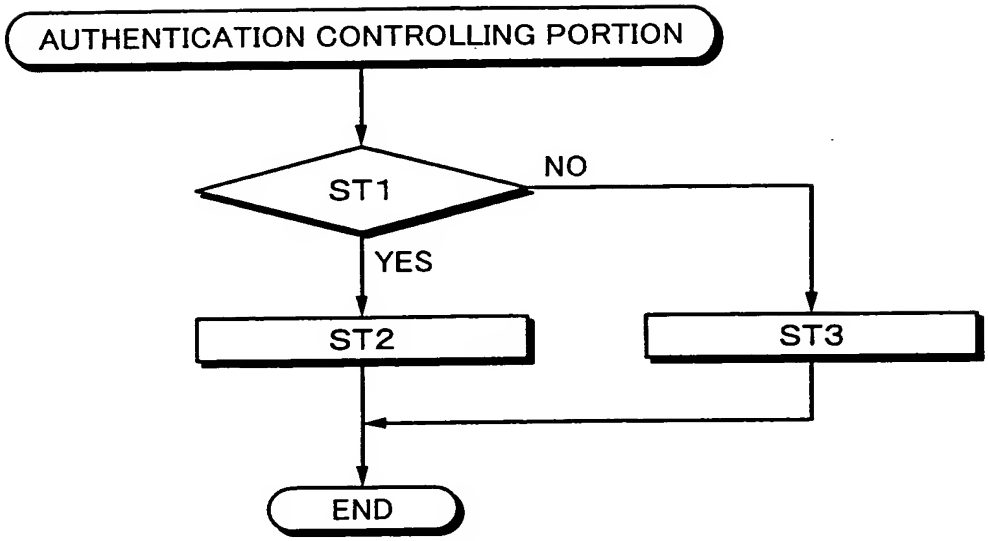


Fig. 5

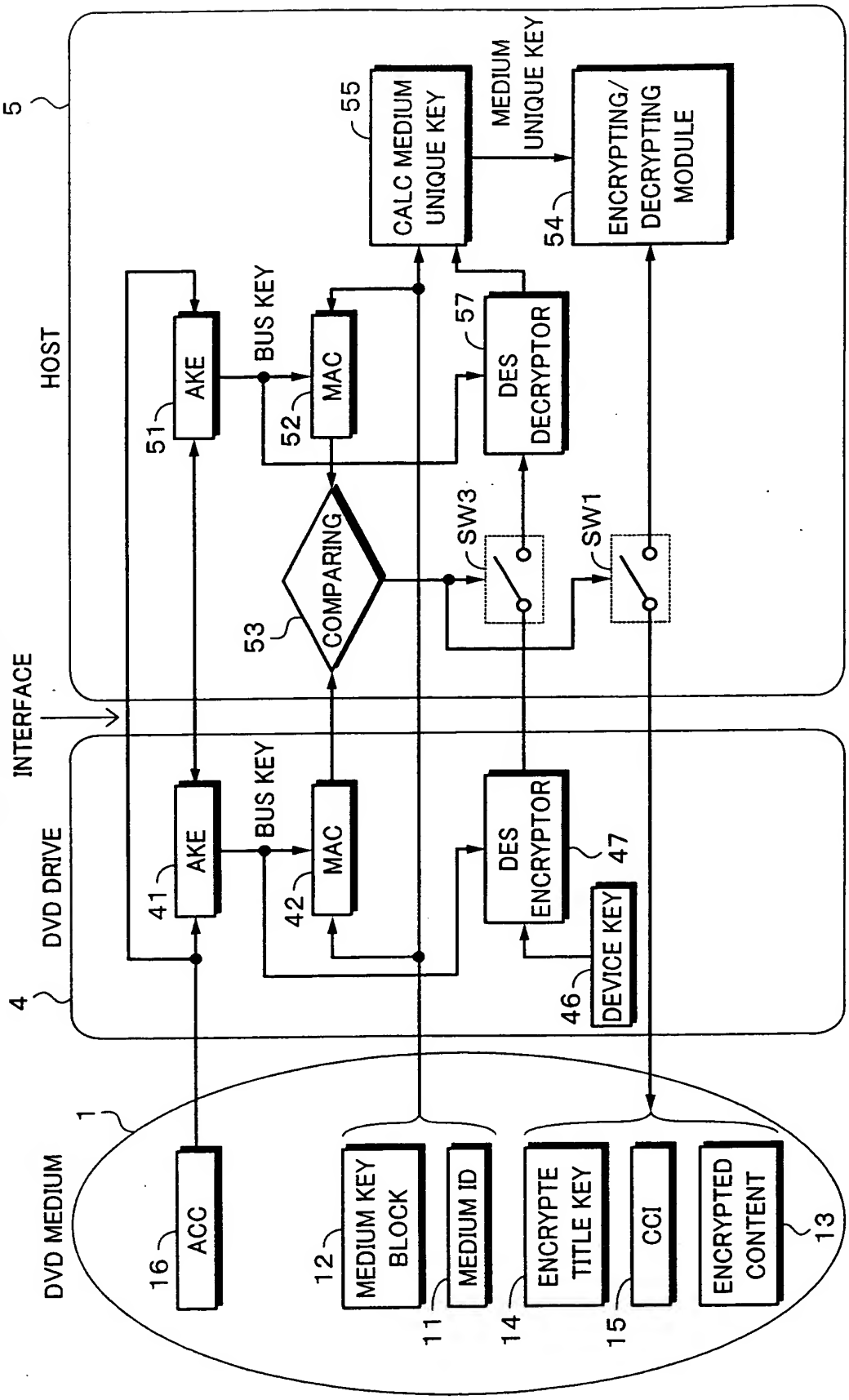

5
HOST
55
CALC MEDIUM UNIQUE KEY
MEDIUM UNIQUE KEY
54
ENCRYPTING/ DECRYPTING MODULE
51
AKE
BUS KEY
52
MAC
57
DES DECRYPTOR
53
COMPARING
SW3
SW1
4a DRIVE – HOST INTERFACE
4
DVD DRIVE
41
AKE
BUS KEY
42
MAC
DES ENCRYPTOR
47
46
DEVICE KEY
1
DVD MEDIUM
16
ACC
12
MEDIUM KEY BLOCK
11
MEDIUM ID
14
ENCRYPTE TITLE KEY
15
CCI
ENCRYPTED CONTENT
13

Fig. 6

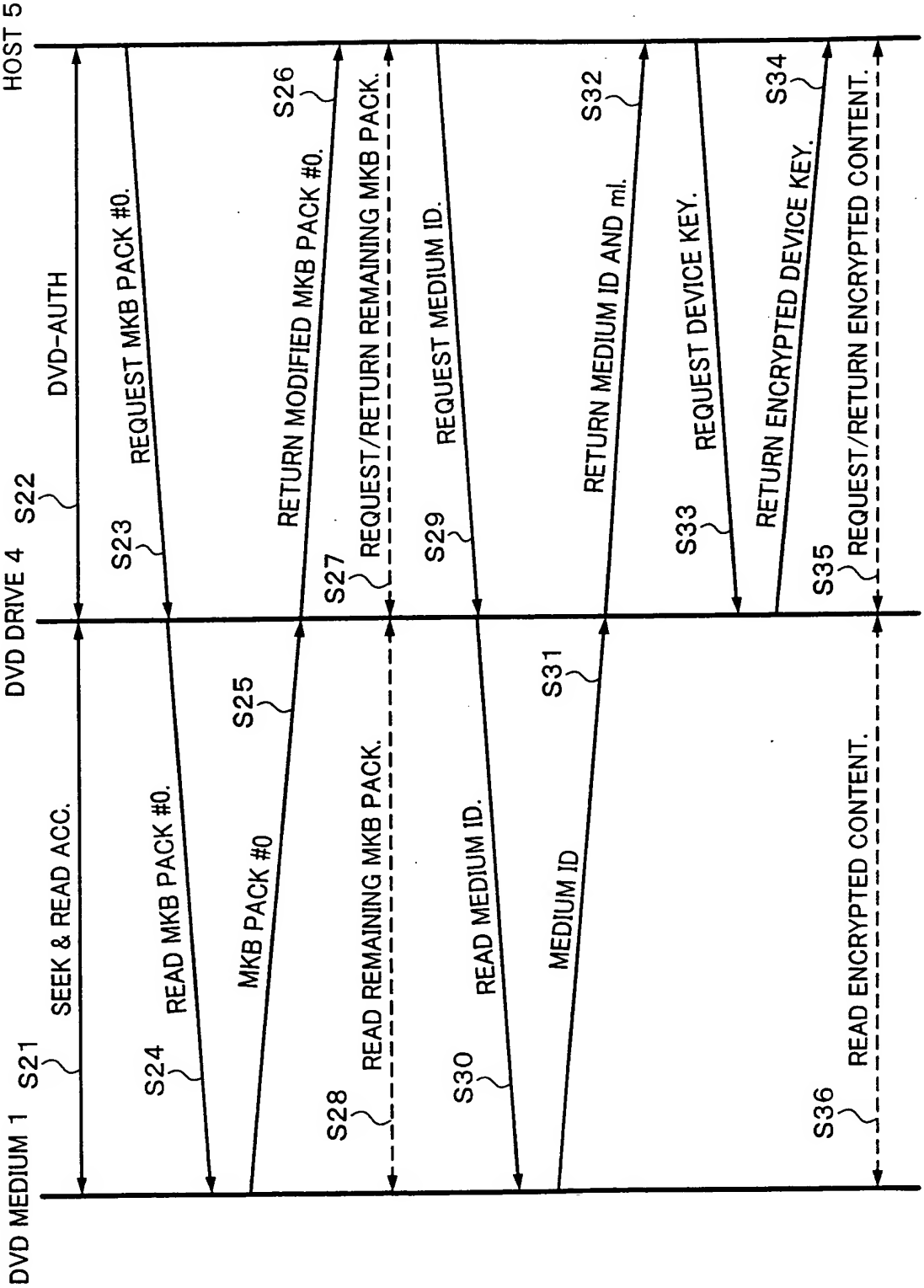

HOST 5
DVD DRIVE 4
DVD MEDIUM 1
DVD-AUTH
S22
REQUEST MKB PACK #0.
S23
RETURN MODIFIED MKB PACK #0.
S26
REQUEST/RETURN REMAINING MKB PACK.
S27
REQUEST MEDIUM ID.
S29
RETURN MEDIUM ID AND ml.
S32
REQUEST DEVICE KEY.
S33
RETURN ENCRYPTED DEVICE KEY.
S34
REQUEST/RETURN ENCRYPTED CONTENT.
S35
SEEK & READ ACC.
S21
READ MKB PACK #0.
S24
MKB PACK #0
S25
READ REMAINING MKB PACK.
S28
READ MEDIUM ID.
S30
MEDIUM ID
S31
READ ENCRYPTED CONTENT.
S36

Fig. 7

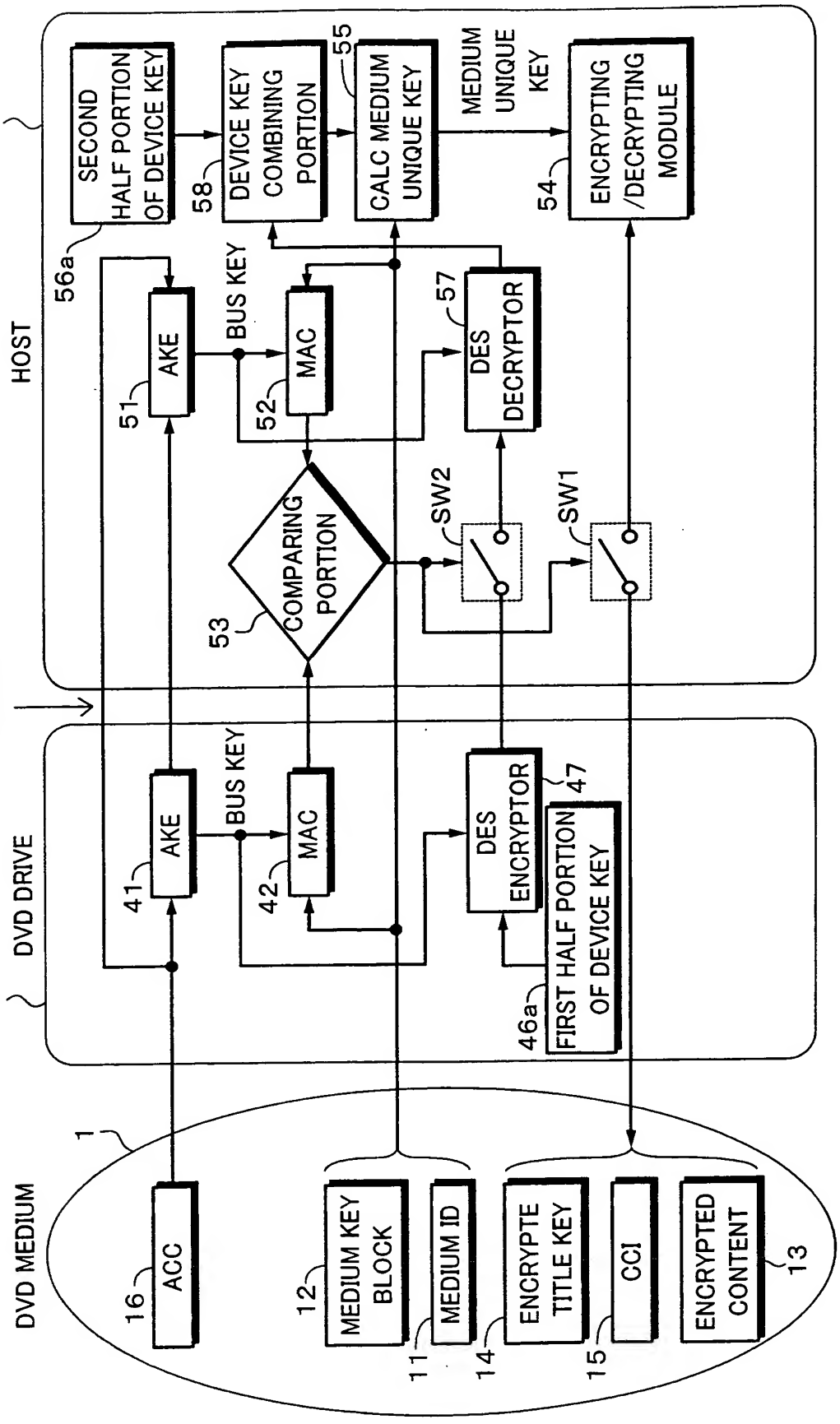

DVD MEDIUM
1
ACC
16
MEDIUM KEY BLOCK
12
MEDIUM ID
11
ENCRYPTE TITLE KEY
14
CCI
15
ENCRYPTED CONTENT
13
4a DRIVE – HOST INTERFACE
4
DVD DRIVE
AKE
41
BUS KEY
MAC
42
DES ENCRYPTOR
47
FIRST HALF PORTION OF DEVICE KEY
46a
5
HOST
AKE
51
BUS KEY
MAC
52
DES DECRYPTOR
57
COMPARING PORTION
53
SW2
SW1
SECOND HALF PORTION OF DEVICE KEY
56a
DEVICE KEY COMBINING PORTION
58
CALC MEDIUM UNIQUE KEY
55
MEDIUM UNIQUE KEY
ENCRYPTING /DECRYPTING MODULE
54

Fig. 8

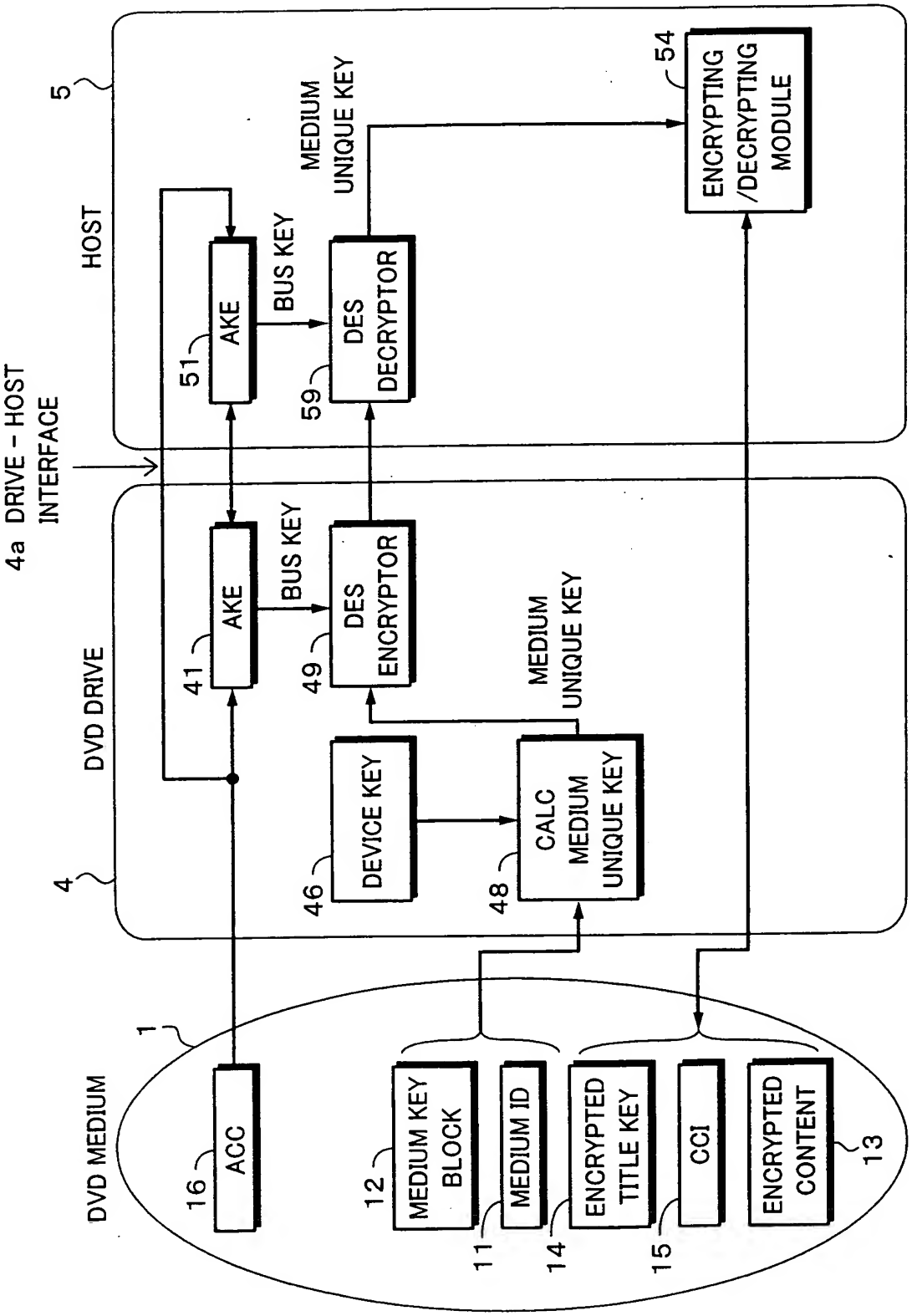

DVD MEDIUM
1
ACC
16
MEDIUM KEY BLOCK
12
MEDIUM ID
11
ENCRYPTED TITLE KEY
14
CCI
15
ENCRYPTED CONTENT
13
4
DVD DRIVE
DEVICE KEY
46
CALC MEDIUM UNIQUE KEY
48
AKE
41
BUS KEY
DES ENCRYPTOR
49
MEDIUM UNIQUE KEY
4a DRIVE – HOST INTERFACE
5
HOST
AKE
51
BUS KEY
DES DECRYPTOR
59
MEDIUM UNIQUE KEY
ENCRYPTING /DECRYPTING MODULE
54

Fig. 9

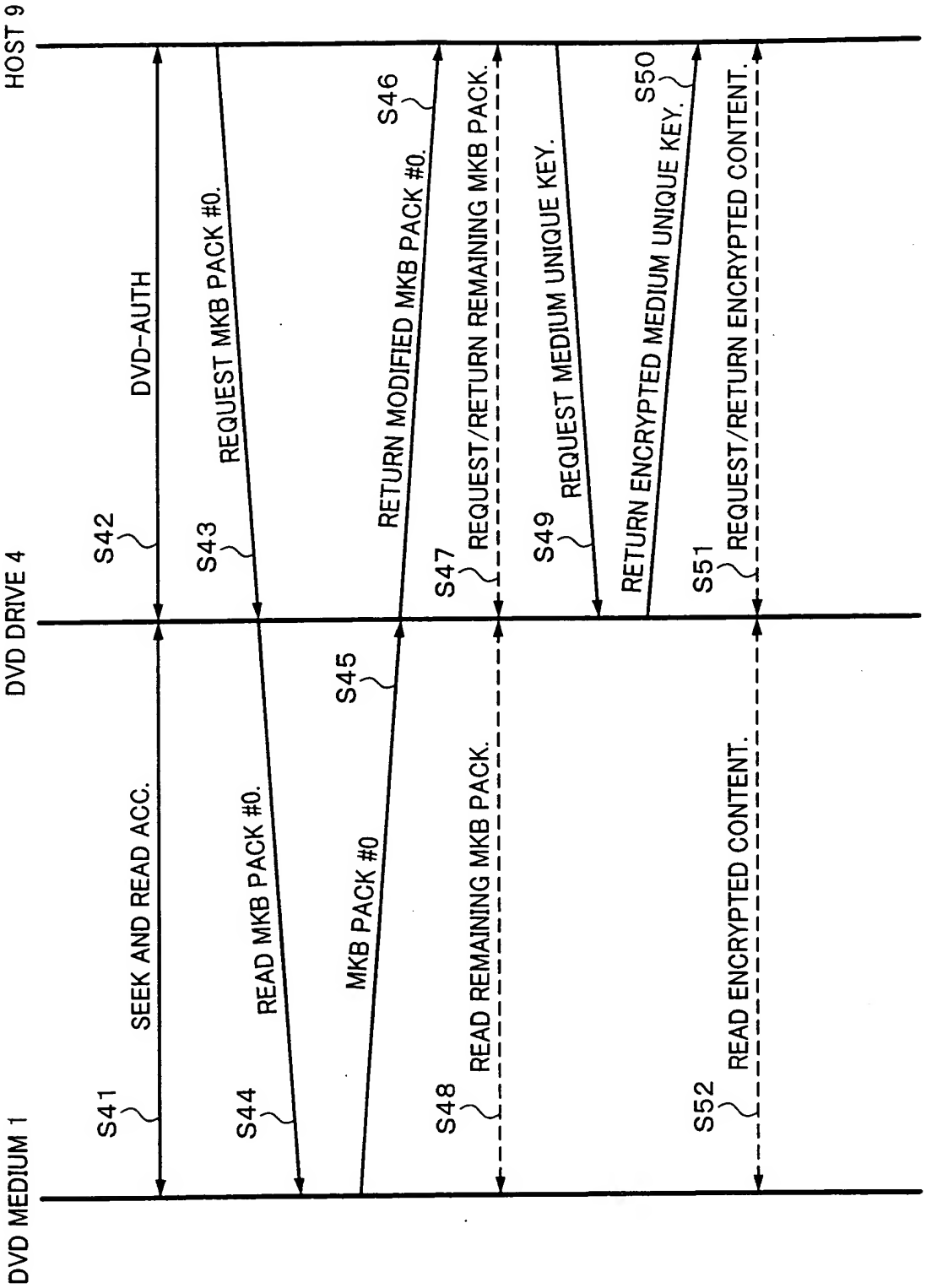

HOST 9
DVD DRIVE 4
DVD MEDIUM 1
S41
SEEK AND READ ACC.
S42
DVD-AUTH
S43
REQUEST MKB PACK #0.
S44
READ MKB PACK #0.
S45
MKB PACK #0
S46
RETURN MODIFIED MKB PACK #0.
S47
REQUEST/RETURN REMAINING MKB PACK.
S48
READ REMAINING MKB PACK.
S49
REQUEST MEDIUM UNIQUE KEY.
S50
RETURN ENCRYPTED MEDIUM UNIQUE KEY.
S51
REQUEST/RETURN ENCRYPTED CONTENT.
S52
READ ENCRYPTED CONTENT.

Fig. 10

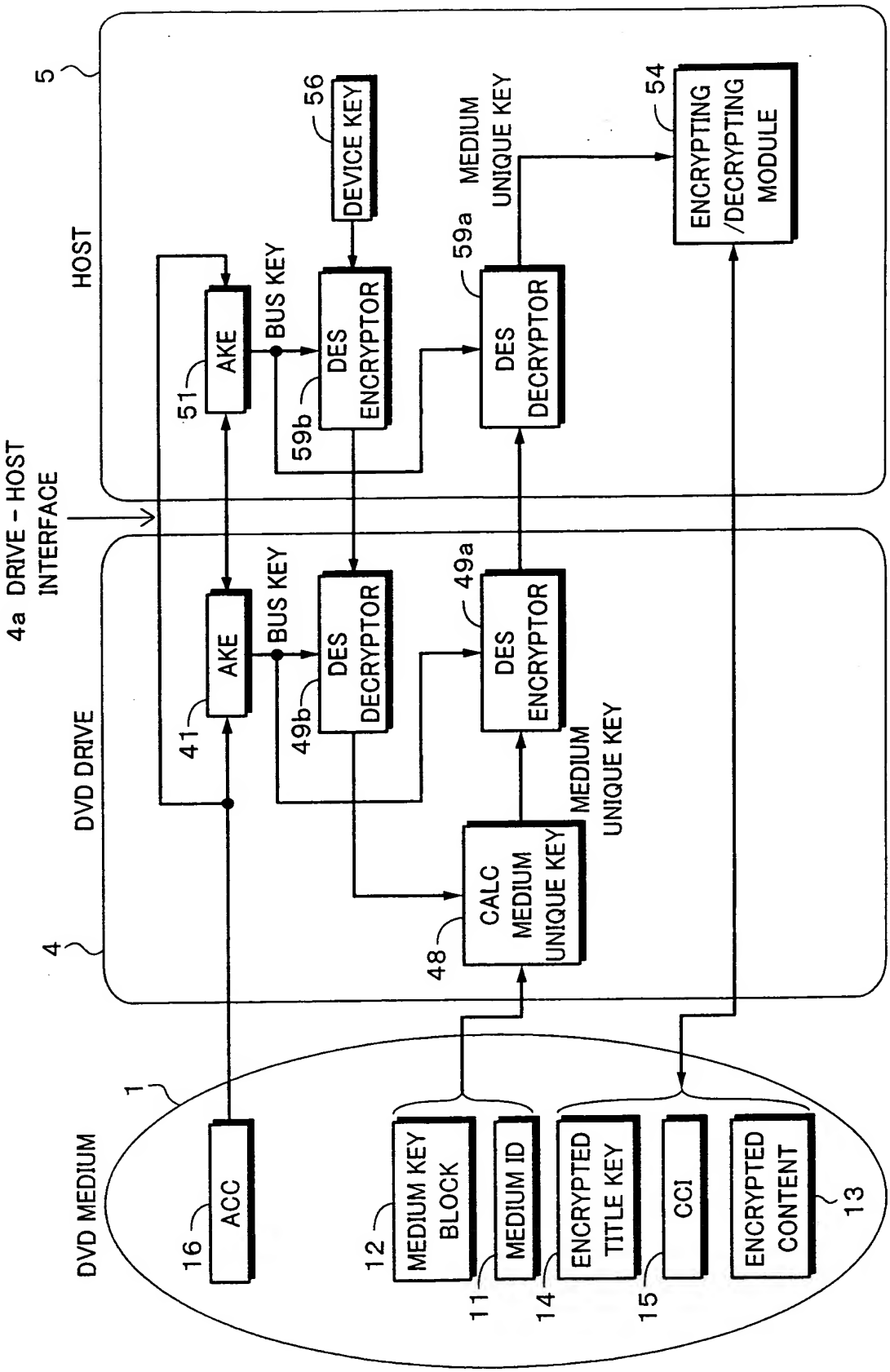

5
HOST
56
DEVICE KEY
54
ENCRYPTING /DECRYPTING MODULE
59a
MEDIUM UNIQUE KEY
BUS KEY
51
AKE
59b
DES ENCRYPTOR
DES DECRYPTOR
4a DRIVE - HOST INTERFACE
DVD DRIVE
4
41
AKE
BUS KEY
49b
DES DECRYPTOR
49a
DES ENCRYPTOR
48
CALC MEDIUM UNIQUE KEY
MEDIUM UNIQUE KEY
DVD MEDIUM
1
16
ACC
12
MEDIUM KEY BLOCK
11
MEDIUM ID
14
ENCRYPTED TITLE KEY
15
CCI
ENCRYPTED CONTENT
13

Fig. 11

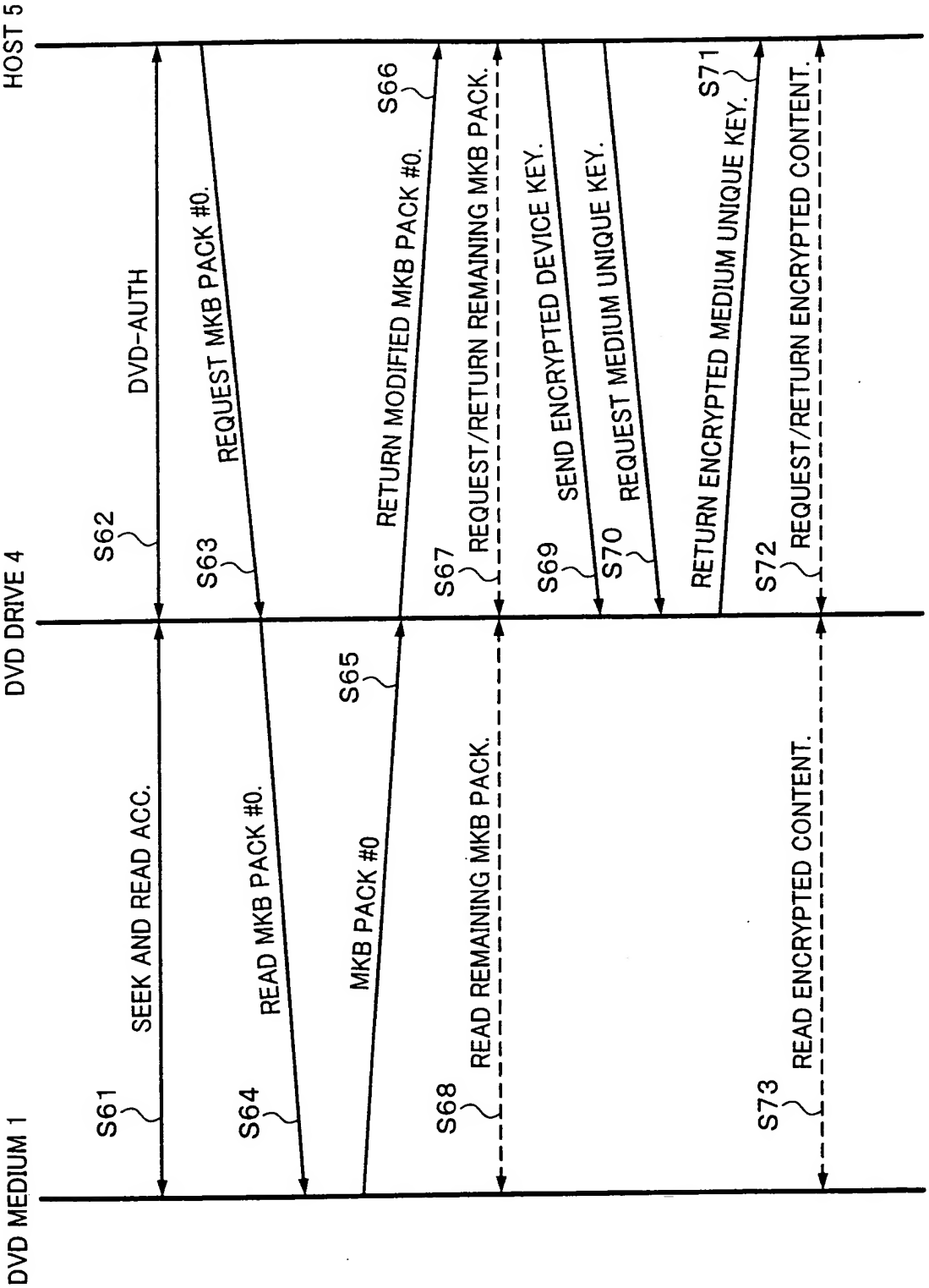

HOST 5
DVD DRIVE 4
DVD MEDIUM 1
S61
SEEK AND READ ACC.
S62
DVD-AUTH
S63
REQUEST MKB PACK #0.
S64
READ MKB PACK #0.
S65
MKB PACK #0
S66
RETURN MODIFIED MKB PACK #0.
S67
REQUEST/RETURN REMAINING MKB PACK.
S68
READ REMAINING MKB PACK.
S69
SEND ENCRYPTED DEVICE KEY.
S70
REQUEST MEDIUM UNIQUE KEY.
S71
RETURN ENCRYPTED MEDIUM UNIQUE KEY.
S72
REQUEST/RETURN ENCRYPTED CONTENT.
S73
READ ENCRYPTED CONTENT.

Fig. 12

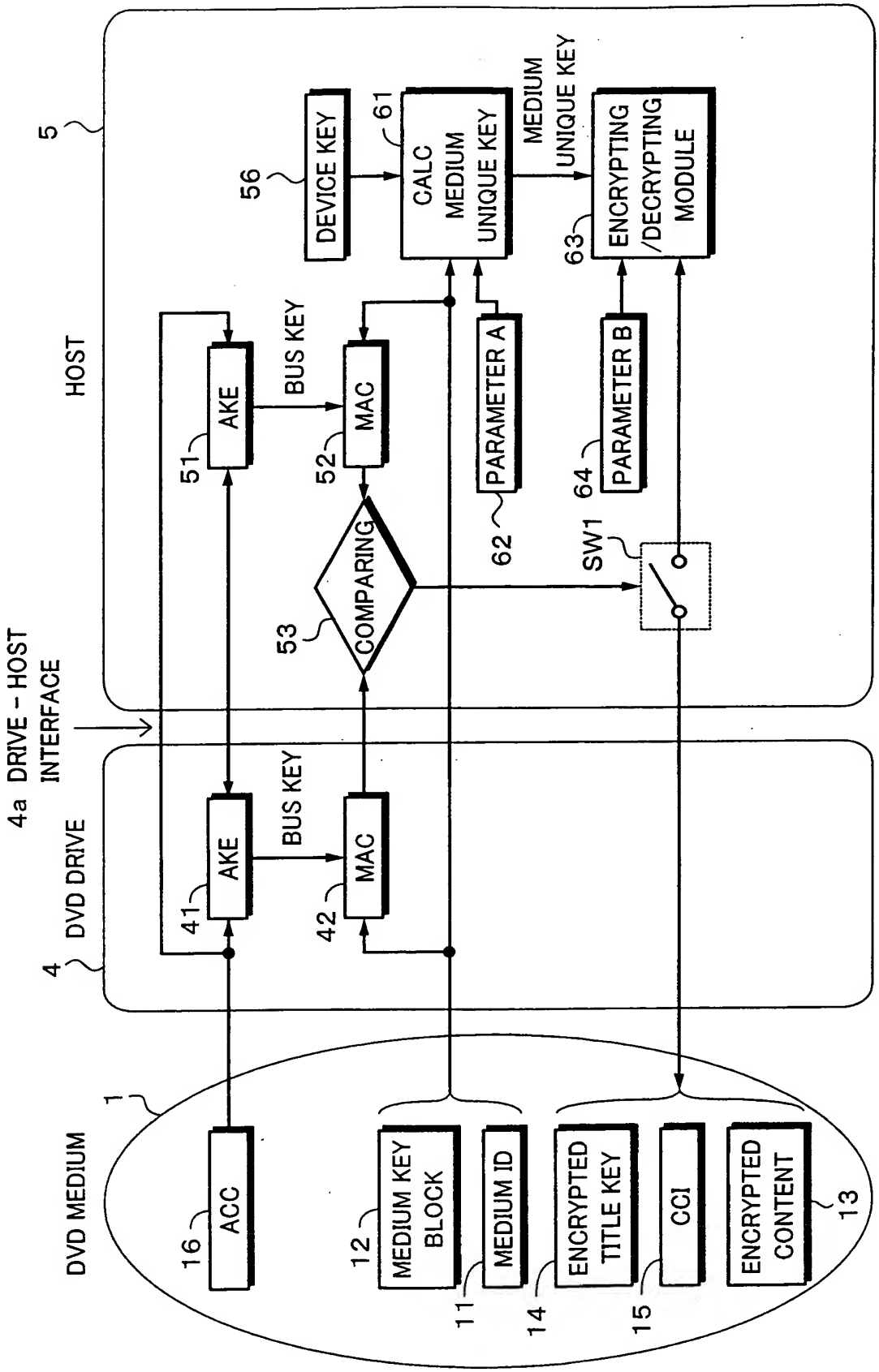

5
HOST
56
DEVICE KEY
61
CALC MEDIUM UNIQUE KEY
MEDIUM UNIQUE KEY
63
ENCRYPTING /DECRYPTING MODULE
BUS KEY
51
AKE
52
MAC
PARAMETER A
62
64
PARAMETER B
SW1
53
COMPARING
4a DRIVE – HOST INTERFACE
4
DVD DRIVE
41
AKE
BUS KEY
42
MAC
1
DVD MEDIUM
16
ACC
12
MEDIUM KEY BLOCK
MEDIUM ID
11
ENCRYPTED TITLE KEY
14
CCI
15
ENCRYPTED CONTENT
13

Fig. 13

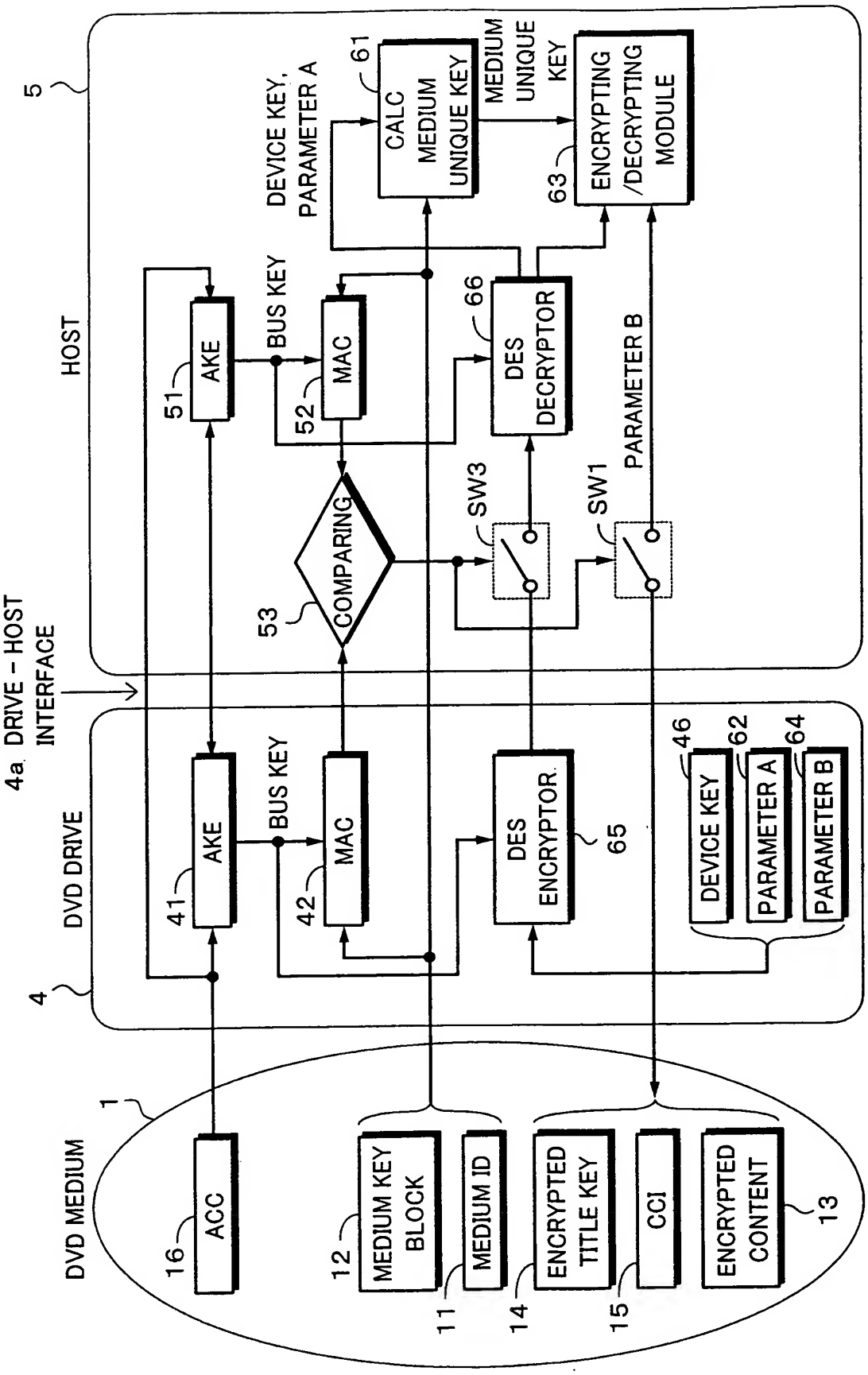

DVD MEDIUM
1
ACC
16
MEDIUM KEY BLOCK
12
MEDIUM ID
11
ENCRYPTED TITLE KEY
14
CCI
15
ENCRYPTED CONTENT
13
4
DVD DRIVE
AKE
41
BUS KEY
MAC
42
DES ENCRYPTOR
65
DEVICE KEY
46
PARAMETER A
62
PARAMETER B
64
4a DRIVE – HOST INTERFACE
5
HOST
AKE
51
BUS KEY
MAC
52
COMPARING
53
SW3
SW1
DES DECRYPTOR
66
PARAMETER B
DEVICE KEY, PARAMETER A
CALC MEDIUM UNIQUE KEY
61
MEDIUM UNIQUE KEY
ENCRYPTING /DECRYPTING MODULE
63

Fig. 14

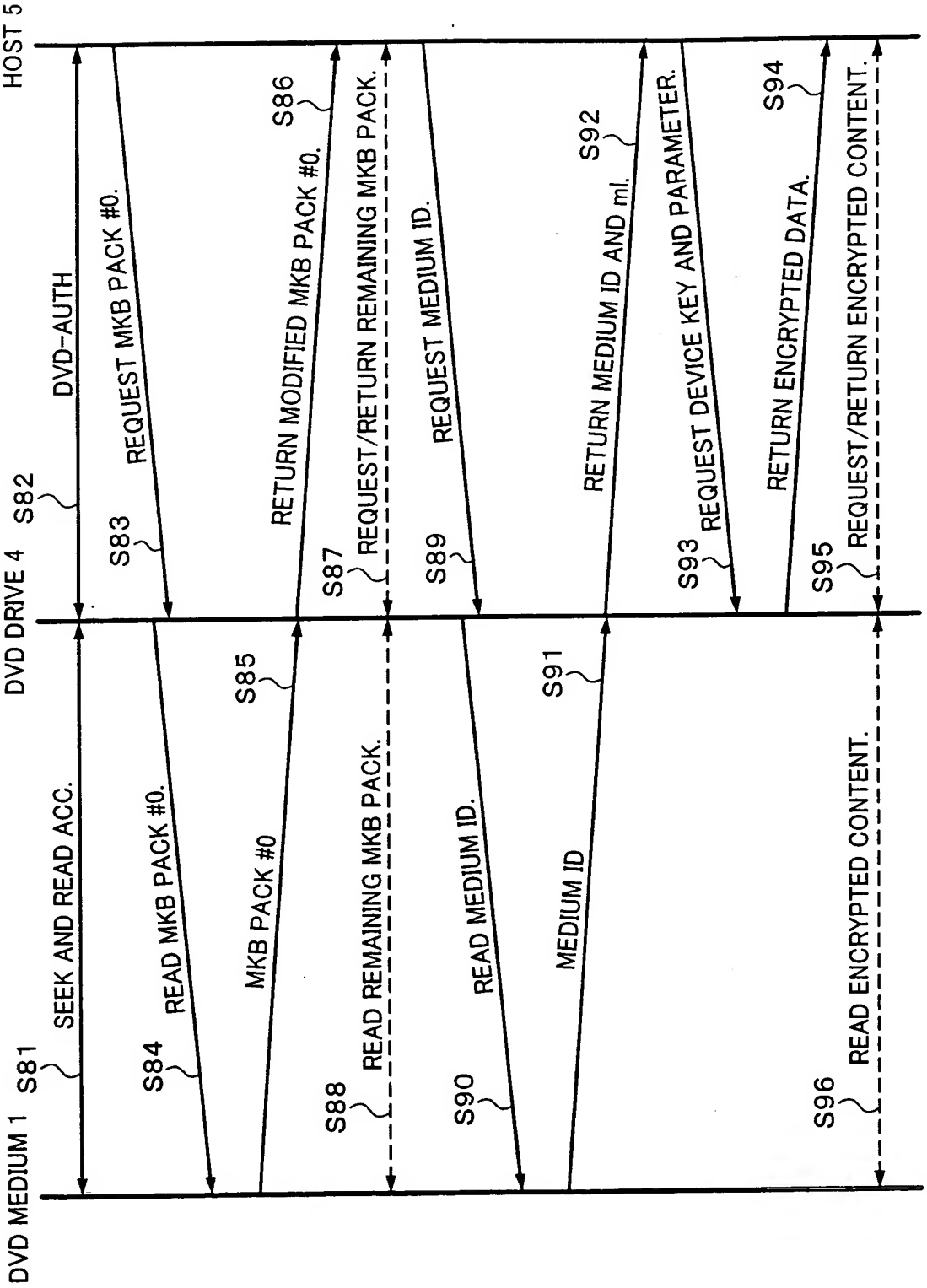

HOST 5
DVD DRIVE 4
DVD MEDIUM 1
S81
SEEK AND READ ACC.
S82
DVD-AUTH
S83
REQUEST MKB PACK #0.
S84
READ MKB PACK #0.
S85
MKB PACK #0
S86
RETURN MODIFIED MKB PACK #0.
S87
REQUEST/RETURN REMAINING MKB PACK.
S88
READ REMAINING MKB PACK.
S89
REQUEST MEDIUM ID.
S90
READ MEDIUM ID.
S91
MEDIUM ID
S92
RETURN MEDIUM ID AND mI.
S93
REQUEST DEVICE KEY AND PARAMETER.
S94
RETURN ENCRYPTED DATA.
S95
REQUEST/RETURN ENCRYPTED CONTENT.
S96
READ ENCRYPTED CONTENT.

Fig. 15

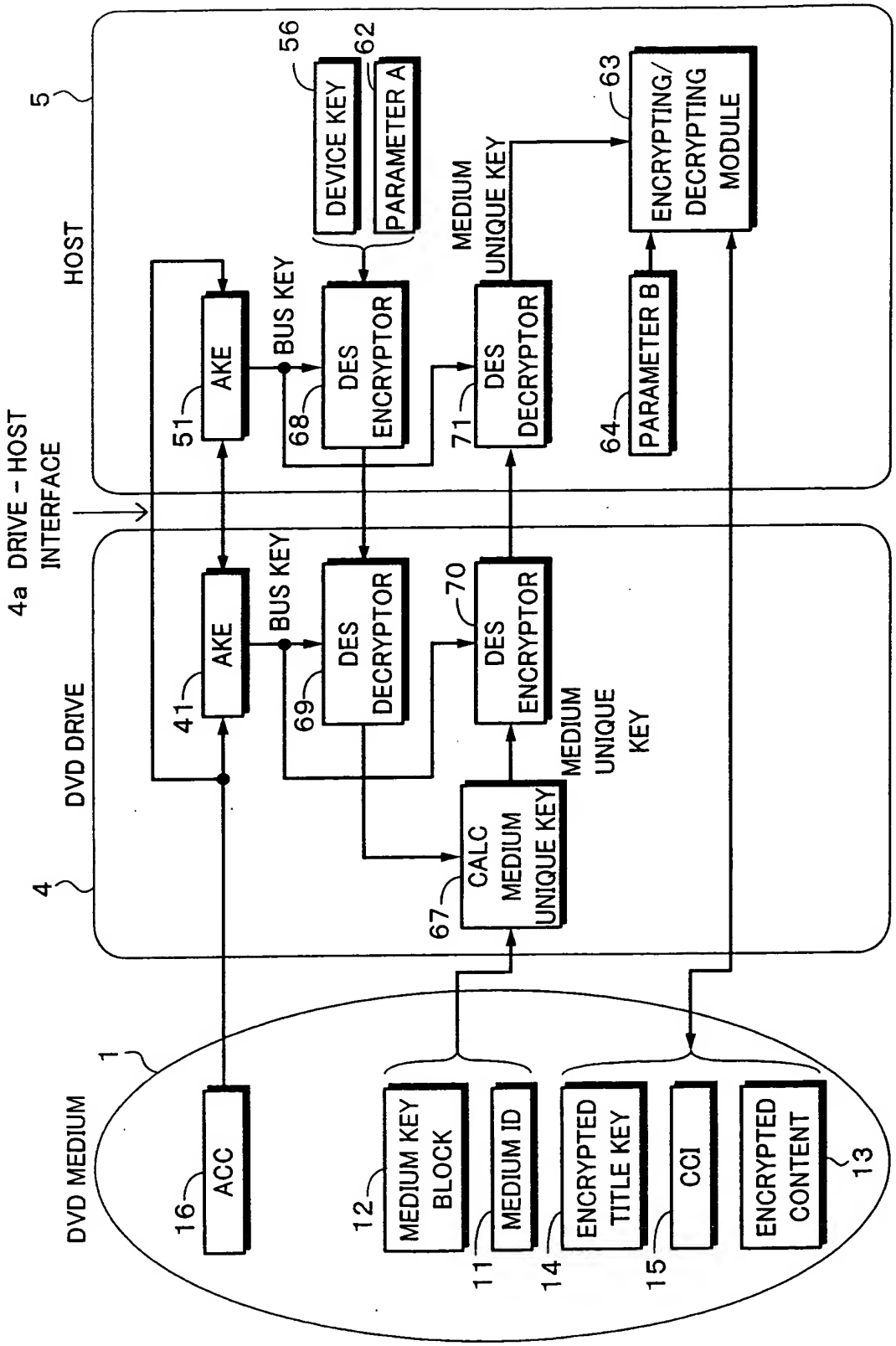

DVD MEDIUM
1
ACC
16
MEDIUM KEY BLOCK
12
MEDIUM ID
11
ENCRYPTED TITLE KEY
14
CCI
15
ENCRYPTED CONTENT
13
4
DVD DRIVE
4a DRIVE – HOST INTERFACE
5
HOST
AKE
41
AKE
51
BUS KEY
BUS KEY
DES DECRYPTOR
69
DES ENCRYPTOR
68
DES ENCRYPTOR
70
DES DECRYPTOR
71
CALC MEDIUM UNIQUE KEY
67
MEDIUM UNIQUE KEY
MEDIUM UNIQUE KEY
DEVICE KEY
56
PARAMETER A
62
PARAMETER B
64
ENCRYPTING/ DECRYPTING MODULE
63

Fig. 16

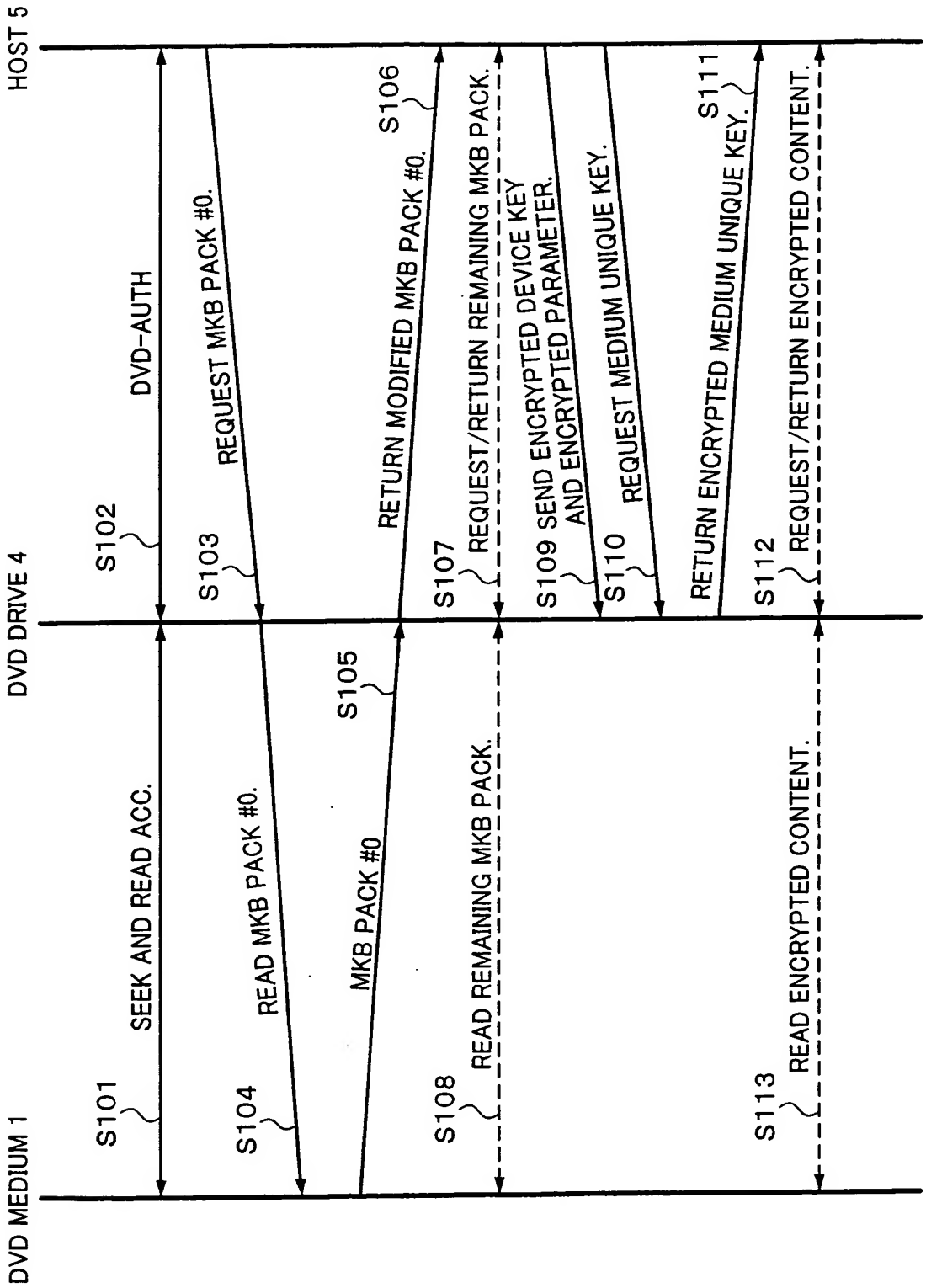

HOST 5
DVD DRIVE 4
DVD MEDIUM 1
S101
SEEK AND READ ACC.
S102
DVD-AUTH
S103
REQUEST MKB PACK #0.
S104
READ MKB PACK #0.
S105
MKB PACK #0
S106
RETURN MODIFIED MKB PACK #0.
S107
REQUEST/RETURN REMAINING MKB PACK.
S108
READ REMAINING MKB PACK.
S109 SEND ENCRYPTED DEVICE KEY AND ENCRYPTED PARAMETER.
S110
REQUEST MEDIUM UNIQUE KEY.
S111
RETURN ENCRYPTED MEDIUM UNIQUE KEY.
S112
REQUEST/RETURN ENCRYPTED CONTENT.
S113
READ ENCRYPTED CONTENT.

Fig. 17

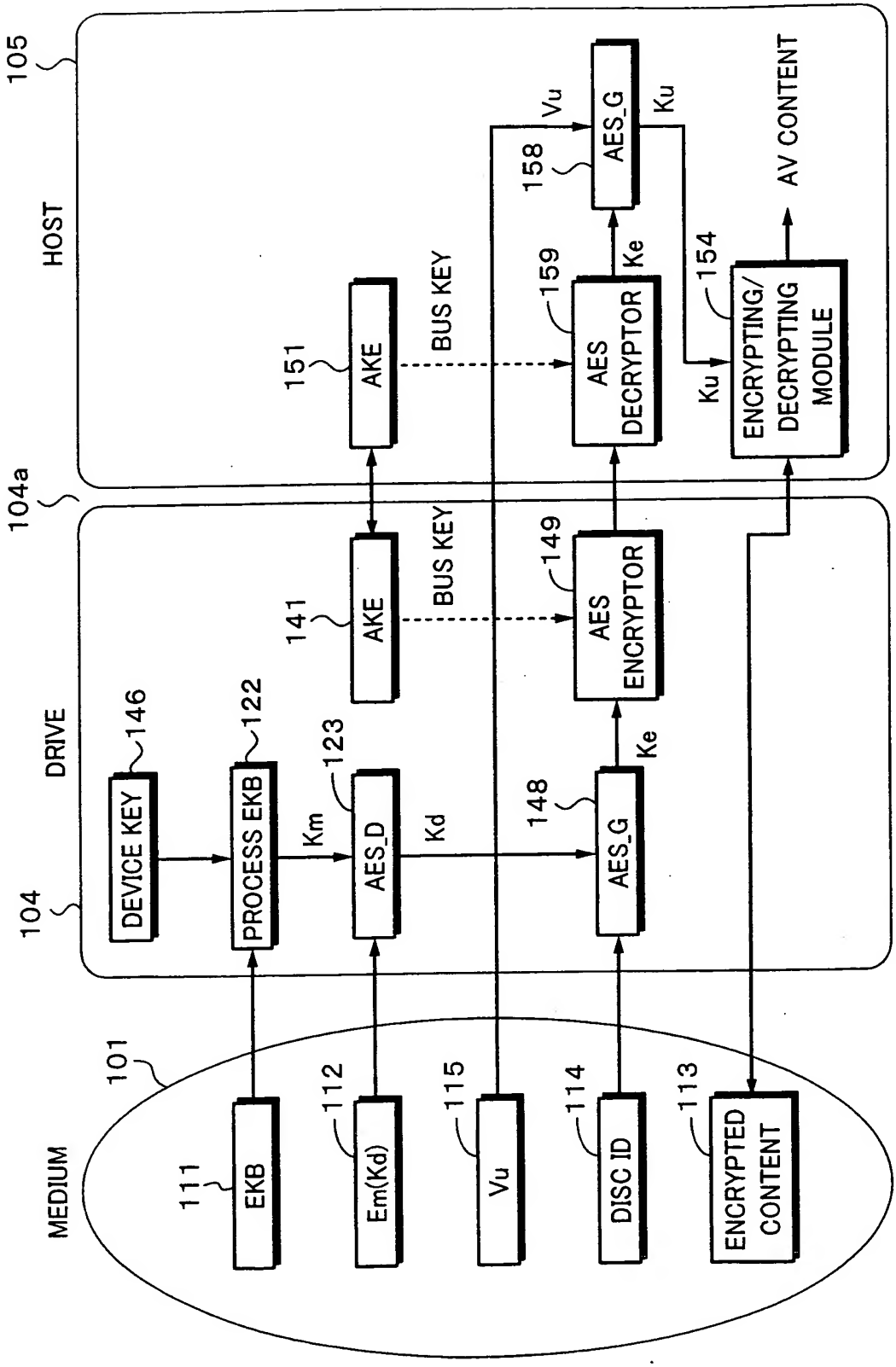
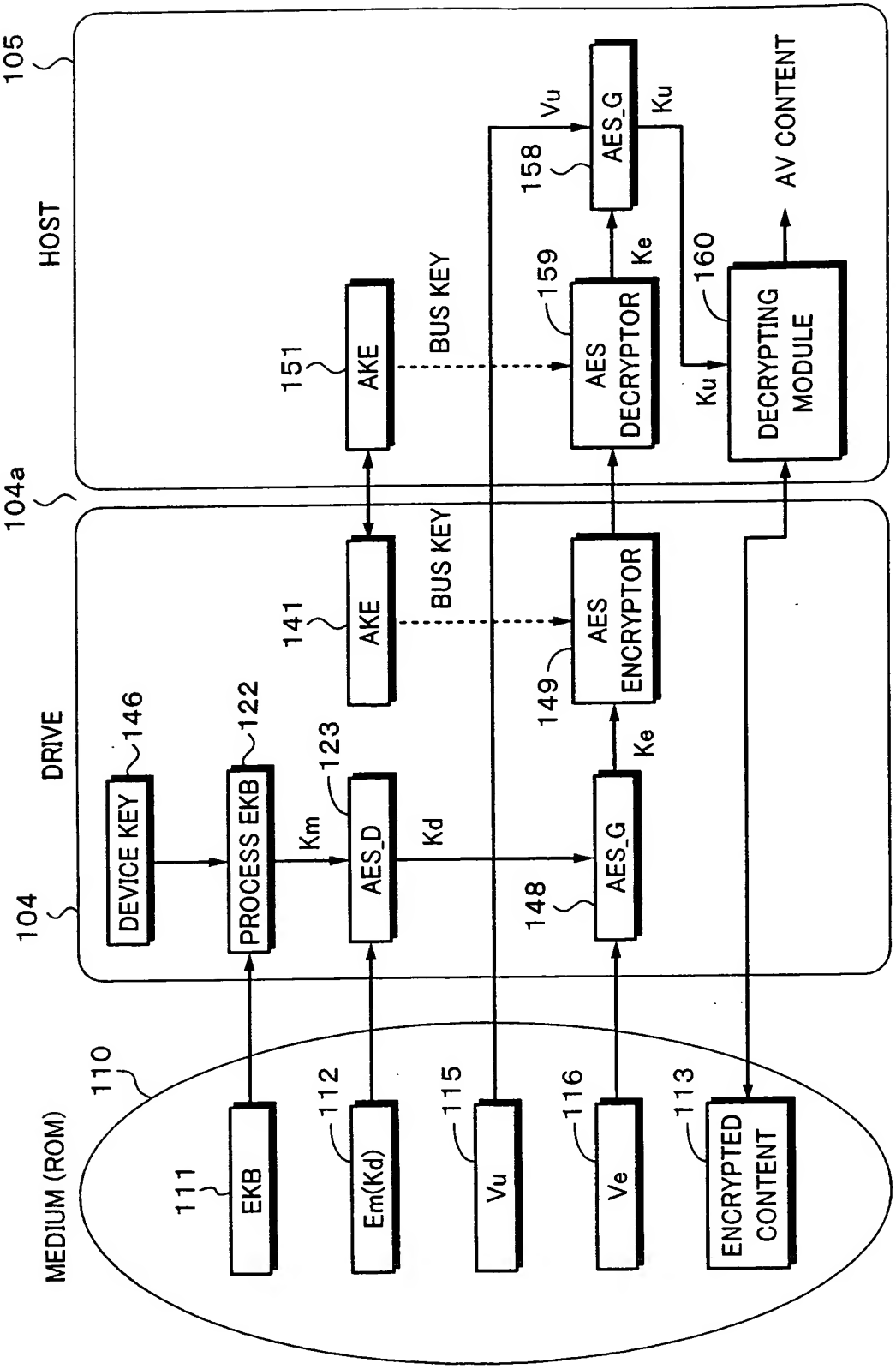

105
HOST
104a
DRIVE
104
MEDIUM
101
DEVICE KEY
146
PROCESS EKB
122
Km
AES_D
123
Kd
AKE
141
BUS KEY
AES ENCRYPTOR
149
AES_G
148
Ke
AKE
151
BUS KEY
AES DECRYPTOR
159
AES_G
158
Vu
Ku
Ke
ENCRYPTING/ DECRYPTING MODULE
154
Ku
AV CONTENT
EKB
111
Em(Kd)
112
Vu
115
DISC ID
114
ENCRYPTED CONTENT
113

Fig. 18


MEDIUM (ROM)
110
111
EKB
112
Em(Kd)
115
Vu
116
Ve
113
ENCRYPTED CONTENT
104
DRIVE
DEVICE KEY
146
PROCESS EKB
122
Km
123
AES_D
Kd
141
AKE
BUS KEY
149
AES ENCRYPTOR
Ke
148
AES_G
104a
105
HOST
151
AKE
BUS KEY
159
AES DECRYPTOR
Ke
158
AES_G
Vu
Ku
160
DECRYPTING MODULE
Ku
AV CONTENT

DESCRIPTION OF REFERENCE NUMERALS

ST1 DO MAC CALCULATED VALUES MATCH ?

ST2 TURN ON SWITCH

ST3 TURN OFF SWITCH

1 DVD MEDIUM 2 RECORDER 3 PLAYER

4 DVD DRIVE 4a INTERFACE 5 HOST

11 MEDIUM ID 12 MEDIUM KEY BLOCK (MKB)

13 ENCRYPTED CONTENT 42, 52 MAC CALCULATING BLOCK

46 DEVICE KEY 46a FIRST HALF PORTION OF DEVICE KEY

47 DES ENCRYPTOR

48 MEDIUM UNIQUE KEY CALCULATING BLOCK

49, 49a DES ENCRYPTOR

49b DES DECRYPTOR 53 COMPARING PORTION THAT COMPARE MACS

54 ENCRYPTING/DECRYPTING MODULE

55 MEDIUM UNIQUE KEY CALCULATING BLOCK

56a SECOND HALF PORTION OF DEVICE KEY 57 DES DECRYPTOR

58 DEVICE KEY COMBINING PORTION 59, 59a DES DECRYPTOR

61 MEDIUM UNIQUE KEY CALCULATING BLOCK

62 PARAMETER A 63 ENCRYPTING/DECRYPTING MODULE

64 PARAMETER B 65 DES ENCRYPTOR

66 DES DECRYPTOR

101 MEDIUM 104 DRIVE 105 HOST

111 EKB 112 ENCRYPTED DISC KEY

113 ENCRYPTED CONTENT 114 DISC ID

115 UNIT KEY GENERATING VALUE 116 EMBEDDED KEY GENERATING VALUE